GF(2)상에서 1차원 Linear Nongroup CA 특성에 관한 연구

조성진[†] · 최언숙[††] · 김한두[†††]

요 약

본 논문에서는 GF(2)상에서 주어진 상태에서 도달불가능한 상태들을 가지는 1차원 선형 nongroup CA의 특성에 관하여 연구한다. 특히 0-tree와 임의의 순환상태 α를 root로 하는 α-tree 사이의 관계들을 밝힌다.

Some Properties of One Dimensional Linear Nongroup Cellular Automata over GF(2)

Sung Jin Cho[†], Un Sook Choi[††] and Han Doo Kim[†††]

ABSTRACT

We investigate some properties of one dimensional linear nongroup cellular automata that have nonreachable states over GF(2). Specially we show interesting relationships between the states in a nonzero tree corresponding to each level state in the 0-tree.

1. 서 론

LFSR의 대안으로 제안 된 cellular automata는 셀들간의 국소적인 상호작용에 의해 랜덤성이 좋은 수열들을 발생시킨다는 것이 알려졌다. 또한 group CA는 전이행렬의 역행렬이 존재하며 특히 특성다항식이 primitive인 경우는 상태 0을 제외한 모든 상태들이 한 사이클을 이루므로 랜덤 패턴 생성 및 여러 분야에 응용되었다[1,5-10]. 그에 비하여 nongroup CA에 대한 연구는 그리 활발하지는 못하였으나 최근 해쉬함수 생성이나 암호, 부울 방정식의 해법, 논리회로의 test에 응용이 되면서 nongroup CA는 관심을 받기 시작하였다.

본 논문에서는 GF(2) 상에서 1차원 선형 nongroup CA가 가지는 여러가지 성질과 0-tree와 임의의 α-tree간의 밀접한 관계가 있음을 밝힌다. 2장에서는 선형 nongroup CA[2-4]의 정의와 간단한 성질들을 밝히고 3장에서는 0-tree와 $\alpha(\neq 0)$-tree 사이의 관계를 보이고 4장에서 결론을 맺는다.

2. 선형 Nongroup CA의 정의 및 성질

선형 nongroup CA에 관한 연구는 group CA에 대한 연구에 비해 그동안 큰 관심을 얻지 못하였으나 최근 nongroup CA가 가지는 몇 가지 흥미로운 성질로 인하여 암호, 해쉬 함수 생성 등 다양한 응용분야에서 이용되고 있다. 이 절에서는 GF(2) 상에서 1차원 선형 nongroup CA의 정의와 몇 가지 특성을 밝힌다.

Group CA는 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA이다. Group CA의 상태 전이 그래프에서 모든 상태들은 유일한 직전자를 가진다. 그리고 임의의 상태에 대한 직전자는 다음과 같이 얻어진다.

본 연구는 2000년도 인제대학교 연구비 지원에 의해서 수행되었음

[†] 정회원, 부경대학교 자연과학대학 수리과학부 재직(교수)
[††] 부경대학교 자연과학대학 응용수학과 대학원(박사과정) 재학중
[†††] 인제대학교 자연과학대학 컴퓨터응용과학부 재직(부교수)

$s^{t-1} = f^{-1} \cdot s^t$

여기서 함수 f는 상태전이 함수이다.

Nongroup CA는 group CA가 아닌 CA로 f^1가 존재하지 않는다. 즉, nongroup CA의 임의의 한 상태에 대한 직전자수는 0이거나 2이상이다. 어떤 상태의 직전자수가 0이란 의미는 직전자가 존재하지 않는 것으로 주어진 상태는 도달불가능한 상태이다. 이와 달리 직전자수가 2이상이란 의미는 주어진 상태가 도달가능한 상태임을 나타내며 직전자가 유일하지 않음을 의미한다. 이처럼 nongroup CA는 현재 상태에서 다음 상태로 가는 함수가 일대일 대응 함수가 아니다. 그러므로 주어진 상태에 대한 역추적이 불가능하다. 다음은 선형 nongroup CA와 앞으로 이 논문의 전개에 필요한 몇 가지 용어들을 정의한다[3].

선형 nongroup CA(LNCA) : Nongroup CA에서 다음 상태를 결정짓는 상태 전이 함수가 XOR 논리로만 이루어져 있어서 이 함수를 행렬로 표현 할 수 있다. 이러한 CA를 선형 nongroup CA(이하 LNCA)라 한다. LNCA에 사용되는 선형 rule은 표 1과 같다.

표 1. 선형 rule

rule	논리식
rule 60	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
rule 90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
rule 102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
rule 150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
rule 170	$q_i(t+1) = q_{i+1}(t)$
rule 204	$q_i(t+1) = q_i(t)$
rule 240	$q_i(t+1) = q_{i-1}(t)$

특성다항식 : 주어진 전이행렬 T에 대하여 특성다항식은 $|T+xI|$이다.

최소다항식 : 특성다항식의 인수 중 T를 근으로 갖는 차수가 가장 낮은 다항식이다.

Attractor : Nongroup CA의 상태 전이 그래프에서 순환상태들 중 사이클의 길이가 1인 상태를 말한다.

α-tree : 순환상태 α를 root로 하는 tree이다.

Depth : Nongroup CA의 상태전이 그래프에서 임의의 한 도달 불가능한 상태에서 가장 가까운 순환상태로 가는데 걸리는 최소의 단계 수를 말한다.

Level : 어떤 상태 x가 α-tree의 level $l(l \le \text{depth})$에 있다는 것은 상태 x가 정확히 l단계 후 상태 α가 되는 위치에 있다는 것이다. 즉, $T^p x = \alpha$가 되는 p값 중 최소 값이 l이다.

r-predecessor : $T^r y = x$을 만족하는 상태 y를 상태 x의 r-predecessor라 한다. $(1 \le r \le 2^n-1)$

Cyclic r-predecessor : 순환상태 x가 속해 있는 cycli에 속한 상태들 중 $T^r y = x$인 상태 y를 나타낸다.

그림 1은 LNCA의 예이다. 4개의 셀로 이루어진 CA에 적용된 rule이 <102,102,102, 60>일 때 전이행렬 T는 아래와 같다.

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

이때 최소다항식(minimal polynomial)은 $m(x) = x^2(x^2+1)$이다. 그림과 같이 tree 구조를 가지는 Nongroup CA는 임의의 도달 가능한 상태에 대하여 직전자가 유일하지 않다. 이는 CA의 임의의 상태에 대한 직전자를 얻을 수 있는 f^1가 존재하지 않음을 말하는 것으로 LNCA에서는 T의 역행렬이 존재하지 않는다. 즉, $det(T)=0$이다. 전이그래프에서 볼 수 있듯이 도달불가능한 상태집합은 {1, 2, 5, 6, 9, 10, 13, 14}이다. 순환상태는 {0}, {8}, {4, 12}이고, attractor는 0과 8이다. 상태 4의 2-predecessor들은 1, 14, 11, 4이고, 1-predecessor들은 3, 12이다. 또한 상태 14와 1은 4-tree의 level 2 상태들이다.
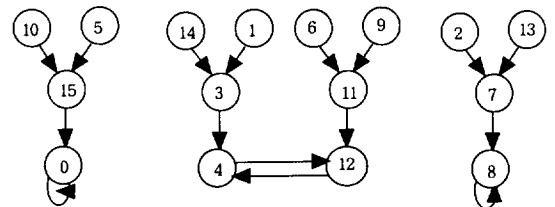
그림 1. 4-cell LNCA의 상태전이 그래프

다음의 몇 가지 정리들은 LNCA의 기본적이며 다음 절에서 제시할 0-tree와 α-tree사이의 관계를 밝히는데 있어 중요한 사실들이다.

보조정리 1> LNCA에서 상태 0은 arrtractor이다.

<증명> 임의의 전이 행렬 T에 대하여 $T0=0$이다. □

LNCA에서 0-tree와 다른 순환상태를 root로 하는 tree는 매우 밀접한 관계를 가지고 있으므로 0-tree에 관한 연구는 필수적이며 매우 중요하다.

보조정리 2> LNCA의 전이행렬 T의 영공간(null space)의 차원이 d이면 상태 0의 직전자의 수는 2^d이다.

<증명> 상태 0의 직전자 x는 $Tx=0$를 만족한다. T의 영공간의 차원이 d이면 이 일차 연립방정식은 자유변수가 d개 존재한다. 자유변수가 가질 수 있는 값이 GF(2)에서 0 또는 1이므로 직전자의 수는 2^d이다. □

정리 1> LNCA에서 도달가능한 상태의 직전자수는 상태 0의 직전자수와 같다.

<증명> 임의의 도달가능한 상태를 α라 하면 α의 직전자 y는 $Ty=\alpha$를 만족한다. α가 도달가능한 상태이므로 $\{y \mid Ty=\alpha\}$는 공집합이 아니다.

그러므로 $|\{y \mid Ty=\alpha\}|\{x \mid Tx=0\}|$이다. □

Nongroup CA의 전이행렬의 최소다항식은 m(x)= $x^d\phi(x)$ 로 나타난다[3]. 여기서 d값은 nongroup CA의 전이그래프에서 depth가 되고, $\phi(x)$가 x^k+1을 나눌 때 k의 최소 값이 nongroup CA의 전이그래프에서 나타나는 사이클들의 길이의 최소공배수가 된다.

보조정리 3> LNCA에서 순환상태의 r-predecessor (r>0)의 수는 상태 0의 r-predecessor의 수와 같다.

<증명> S_r을 상태 0의 r-predecessor의 집합이라 하자(r>0). 그러면 S_r은 다음과 같이 표현된다.

$S_r=\{y \mid T^r y=0\}$.

또 X_0를 0이 아닌 임의의 한 순환상태라 하고 A_r을 X_0의 r-predecessor의 집합이라 하면 A_r은 다음과 같이 표현된다.

$A_r=\{z \mid T^r z=X_0\}$.

X_0가 순환상태이므로 X_0가 놓여 있는 cycle에 있는 상태 중 하나는 반드시 X_0의 r-predecessor가 되므로 $A_r \neq \varnothing$이다.

그러므로 $|S_r|=|A_r|$이다. □

정리 2[3]> LNCA에서 임의의 α-tree의 구조는 0-tree의 구조와 동형이다.

<증명> 정리1에 의해 α-tree의 도달가능한 상태의 직전자수는 상태 0의 직전자수와 같다. 또한 보조정리3>에 의해 임의의 순환상태의 r-predecessor의 수가 모두 같으므로 α-tree의 각 level의 상태수는 0-tree의 각 level의 상태수와 모두 같다. 그러므로 두 tree는 동형이다. □

3. 선형 Nongroup CA에서 순환상태들의 tree와 0-tree와의 관계

LNCA의 상태전이그래프에서 α-tree의 구조는 0-tree와 동형이다[3]. 그러므로 α-tree와 0-tree사이의 관련성을 밝히는 것은 LNCA의 행동을 분석하는데 있어 매우 중요한 문제이다. 이 절에서는 1차원 LNCA의 0-tree와 $\alpha(\neq 0)$-tree의 상태들간의 관계들을 밝힘으로 서로 대응되는 상태들을 찾을 수 있고, LNCA를 보다 효율적으로 분석할 수 있음을 보인다.

다음 정리에 의해서 0-tree의 상태의 수를 알 수 있다.

정리 3> LNCA의 상태전이그래프에서 0-tree의 depth를 d라 하고 주어진 전이행렬 T의 영공간의 차원이 r이면 0-tree의 상태의 수는 2^{rd}이다.

<증명> 전이행렬의 T의 영공간의 차원이 r이므로 보조정리2와 정리1에 의해 임의의 도달가능한 상태의 직전자수는 2^r개다. a_i를 0-tree의 level i에 있는 상태들의 수라 하면 $a_{i+1}=2^r a_i$이다. 따라서 0- tree의 level i에 있는 상태들의 수는 $(2^r)^{i-1}(2^r-1)$이다. 그러므로 0-tree에 속해있는 상태들의 수는 다음과 같다.

$$1+(2^r-1)+2^r(2^r-1)+\cdots+(2^r)^{d-1}(2^r-1)$$
$$=1+\frac{(2^r-1)\{(2^r)^d-1\}}{2^r-1}$$
$$=1+(2^{rd}-1)=2^{rd}$$ □

보조정리 4> 도달가능한 상태의 직전자의 수가 r인 LNCA에서, 상태 0의 i-predecessor를 P_1, P_2,

$P_3, \cdots, P_{r^i}$라 하고, 도달가능한 0이 아닌 임의의 상태 X의 i-predecessor중 하나를 X_1이라 하면 X의 i-predecessor 집합은 다음과 같다.

$\{X_1 \oplus P_j \mid j=1,2,3,\cdots,r^i\}$

(단, $\oplus$는 bitwise 덧셈연산)

<증명> 우선 B_i를 상태 0의 i-predecessor의 집합이라 하면 집합 B_i는 다음과 같다.

$B_i = \{Y | T^i Y = 0\} = \{P_1, P_2, \cdots, P_{r^i}\}$ 여기서 $P_1 = 0$이다. 그리고 상태 X의 i-predecessor의 집합을 Q_i라 하면 $Q_i = \{Y \mid T^i Y = X\}$이다. 상태 X_1이 X의 i-predecessor이므로 $X_1 \in Q$이다.

$Q \neq \emptyset$ 이므로, $|Q| = |P| = r^i$이다. 한편

$$T^i(X_1 \oplus P_j) = T^i X_1 \oplus T^i P_j = T^i X_1 \oplus 0 = X$$

이므로 $X_1 \oplus P_j$, $(j=1,2,\cdots,r^i)$가 X의 i-predecessor이다.

그러므로 X의 i-predecessor집합 Q_i는

$\{X_1 \oplus P_j \mid j=1,2,3,\cdots,r^i\}$이다. □

정리 4> 상태 0의 직전자 수가 r일 때, P_{ij}를 0-tree의 level i의 j번째 상태라 하고, R_i를 상태 X의 cyclic i-predecessor라 하자. 그리고 X_{ij}를 X-tree의 level i의 j번째 상태라 하면 X_{ij}는 다음을 만족한다.

$X_{ij} = R_i \oplus P_{ij}$ .... (*)

(단, $\oplus$는 bitwise 덧셈연산,

$1 \le i \le \text{depth}$, $j = 1, \cdots, (r-1)r^{i-1}$)

<증명> 위 식(*)을 수학적 귀납법으로 증명한다.

먼저 $i=1$ 인 경우는 보조정리4>에서 i가 1인 경우이므로 성립한다.

$i=k$인 경우도 성립한다고 가정하면 $|\{X_{kj}\}| = |\{R_k \oplus P_{kj}\}|$고 $X_{kj} = R_k \oplus P_{kj}$ ($j=1,2,\cdots,$) $(r-1)r^{i-1}$)이다.

$i=k+1$에 대하여

$T(X_{k+1j} \oplus R_{k+1}) = X_{kj} \oplus R_k = P_{kj}$이다.

그러므로 $X_{k+1j} \oplus R_{k+1}$은 P_{kj}의 직전자 중 하나인 P_{k+1j}이다.

따라서 $X_{k+1j} \oplus R_{k+1j} = P_{k+1j}$ 이고

$X_{k+1j} = R_{k+1j} \oplus P_{k+1j}$ 이다. 그러므로 식 (*)은 $k=i+1$인 경우에도 성립한다. □

정리 5> X_l, X_m이 X-tree의 level i의 상태이고 j번 단계 후 비로소 두 상태가 같은 상태가 될 때, 즉 $T^k X_l = T^k X_m$인 최소의 k값이 $j(\le i)$일 때 $X_l \oplus X_m$는 0-tree의 level j상태 중 하나이다.

<증명> $T^j X_l = T^j X_m$이므로

$T^j(X_l \oplus X_m) = 0$ 이다. 이는 $X_l \oplus X_m$가 상태 0의 j-predecessor임을 의미한다. $X_l \oplus X_m$가 0-tree의 level $p(<j)$의 상태라면 $T^p(X_l \oplus X_m) = 0$이고 $T^p X_l = T^p X_m$이 되어 가정에 모순이 된다. 그러므로 $X_l \oplus X_m$는 0-tree의 level j 상태 중 하나이다. □

위의 정리로부터 다음의 따름정리를 얻을 수 있다.

따름정리 1[3]> 임의의 도달가능한 상태의 서로 다른 직전자의 합은 상태 0의 0이 아닌 직전자이다.

4. 결 론

CA는 LFSR보다 난수성이 강하므로 암호화에 있어 보다 효율적으로 혼돈과 확산이 이루어진다. 그러나 이를 분석함은 상당한 어려움이 따른다. 본 연구는 암호 알고리즘 개발 및 해쉬 함수 생성에 응용되고 있는 nongroup CA의 성질을 밝혔다. 특히 GF(2)상에서 1차원 LNCA의 성질과 순환상태를 root로 하는 tree들 사이의 관계를 밝힘으로써 CA를 이용한 암호알고리즘의 분석에 있어서 도움이 되리라 사료된다.

참 고 문 헌

[1] P.H. Bardell, "Analysis of cellular automata used as pseudorandom pattern generators", *Proc. IEEE int. Test. Conf.*, 1990, pp. 762~767

[2] S. Bhattacharjee, S. Sinha, C. Chattopadhyay, P.P. Chaudhuri "Cellular automata based scheme for solution of Boolean equations", *IEEE Proc.-Comput. Digit. Tech*, **Vol. 143, No. 3,** 1996, pp. 174~180.

[3] S. Chattopadhyay, *Some studies on Theory and Applications of Additive Cellular Automata*, Ph.D. Thesis, I.I.T., Kharagpur, India, 1996.

[4] S. Chakraborty, D.R. Chowdhury, Chaudhuri, "Theory and Application of nongroup cellular automata for synthesis of easily testable finite state machines", *IEEE. Trans. Computers*, **Vol. 45, No. 7**, 1996, pp. 769~781

[5] P.P. Chaudhuri, D.R. Chowdhury, S. Nandy and Chattopadhyay, *Additive Cellular Automata Theory and Application*, **1**, IEEE Computer Society Press, California, 1997.

[6] A.K. Das and P.P. Chaudhuri, "Efficient characterization of cellular automata", *Proc. IEE (Part E)*, **Vol. 137, No.1**, 1990, pp. 81~87

[7] A.K. Das and P.P. Chaudhuri, "Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation", *IEEE Trans. Comput.*, **Vol. 42**, 1993, pp. 340~352

[8] S. Nandi and P.P. Chaudhuri, "Analysis of Periodic and Intermediate Boundary 90/150 Cellular automata", *IEEE Trans. Computers*, **Vol. 45, No 1**, 1996, pp. 1~12

[9] S. Nandi, B.K. Kar and P.P. Chaudhuri, "Theory and Application of Cellular Automata in Cryptography", *IEEE Trans. Computers*, **Vol. 43**, 1994, pp. 1346~1357

[10] M. Serra, T. Slater, J.C. Muzio and D.M. Miller, "The analysis of one dimensional linear cellular automata and their aliasing properties", *IEEE Trans Computer-Aided Design*, **Vol. 9**, 1990, pp. 767~778

조 성 진

1979년 강원대학교 수학교육과 (이학사)
1981년 고려대학교 수학과 대학원(이학석사)
1988년 고려대학교 수학과 대학원(이학박사)
1988년~현재 부경대학교 자연과학대학 수리과학부 재직(교수)
관심분야 : Cellular Automata론, ATM, Queueing론

최 언 숙

1992년 성균관대학교 산업공학과 (공학사)
2000년 부경대학교 자연과학대학 응용수학과 대학원(이학석사)
2000년~현재 부경대학교 자연과학대학 응용수학과 대학원(박사과정) 재학중
관심분야 : Cellular Automata론, ATM, Queueing론

김 한 두

1982년 고려대학교 수학과(이학사)
1984년 고려대학교 수학과 대학원(이학석사)
1988년 고려대학교 수학과 대학원(이학박사)
1989년~현재 인제대학교 자연과학대학 컴퓨터 응용과학부 재직(부교수)
관심분야 : 전산수학, Cellular Automata론